RAISECOM
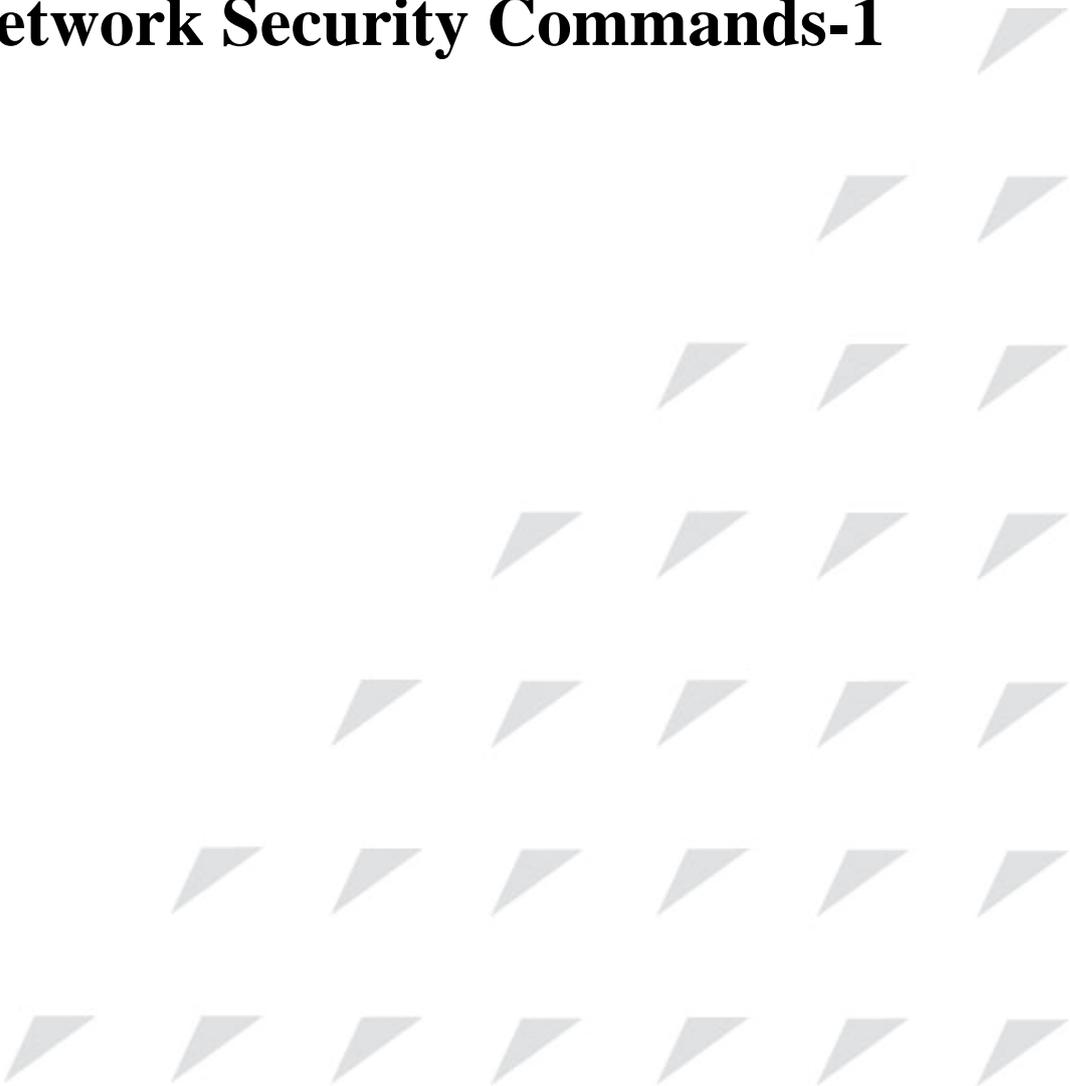
www.raisecom.com

ACL and Network Security Commands-1

CONTENTS

Chapter 1   ACL and Network Security Commands

1.1 ip-access-list

[Function]

Set IP access control list, use **no** to delete this operation.

[Command Format]

ip-access-list *<0-399> (deny | permit) (ip|tcp|udp|icmp|igmp|<0-255>) (A.B.C.D A.B.C.D | any)
[<1-65535>] (A.B.C.D A.B.C.D | any) [<1-65535>]*

[Parameter]

0-399: serial number for IP Access Control List.

permit: Permit access if conditions are matched.

deny:Deny access if conditions are matched.

protocol: define protocol type in the packet head. Protocol type can be icmp, igmp, tcp, udp, ip,
protocol number from 0-255, if set the value to IP or 0, it stands for all IP packets.

A.B.C.D A.B.C.D | any: The first A.B.C.D denotes source IP address, the second A.B.C.D
denotes mask of source address, all of them use dotted decimal notation; **any** stands for all the
source IP address.

1-65535: it is the port number of TCP or UDP source packet, 1~65535.

A.B.C.D A.B.C.D | any: The first A.B.C.D denotes destination IP address, the second A.B.C.D
denotes mask of destination address, all of them use dotted decimal notation; **any** stands for all
of the destination IP address.

1-65535: it is the port number of TCP or UDP destination packet, 1~65535.

[Command Modes]

Global configuration mode; Privileged user.

[Executing Command Instruction]

Use this command to define an IP ACL, the parameter *permit | deny* is used to permit or deny
the access of packets. This command only set the data filter conditions, and need to be applied
to physical port or VLAN to let it be effective.

[Explanation of command execution echo]

The mask is wrong.

Set successfully

Set unsuccessfully

[Example]

Deny terminal device with source address 192.168.1.19 to ping other terminal device:

Raisecom (config)#**ip-access-list** *50* **deny icmp** *192.168.1.19 255.255.255.255 **any***

[Related commands]

Commands	Description
no ip-access-list (*{0-399}*/**all**)	Delete all IP ACL entries.
show ip-access-list [*{0-399}*]	Show all the IP ACL entries.

1.2 ip ip-access-list

[Function]

The command is used to add the filter rule into layer-3 interface, use **no** command to delete filtering rule.

[Command format]

[no] ip ip-access-list (*all* | *{0-199}*)

[Parameter]

ip-access-list: IP access list.

all |{0-399}: the serial number of ACL, if it is "*all*", then it means all defined IP ACL.

[Command mode]

Ethernet layer-3 interface mode; Privileged user.

[Executing Command Instruction]

Use this command to apply one or more previously defined IP ACL to layer-3 interface. The filter rule is composed by IP ACL defined before. The add order of match rules when configuring filter determine the priority of the rules. The later added rules are of the higher priority. If the rules are conflict when configuring calculation, the order follows priority level order.

The previously defined IP ACL applies on layer-3 interface, and will be effective when receives packets.

[Explanation of command execution echo]

Set access list XX failed

[Example]

Raisecom(config)# **ip ip-access-list** *0*

[Related commands]

Commands	Description
show interface ip ip-access-list	Show layer-3 access control configuration.
ip-access-list	IP access list configuration.

1.3 show interface ip ip-access-list

[Function]

This command is used to show access control related information for layer-3 interface.

[Command format]

show interface ip ip-access-list

[Command Modes]

Privileged user.

[Executing Command Instruction]

This command is used to show related information of layer-3 ACL. The information shown is based on the order of arrival, the later the information is added, the more frontal it is.

[Explanation of command execution echo]

Filter list(Larger order number, Higher priority):

Index   ACL-Index

--

0   IP   3